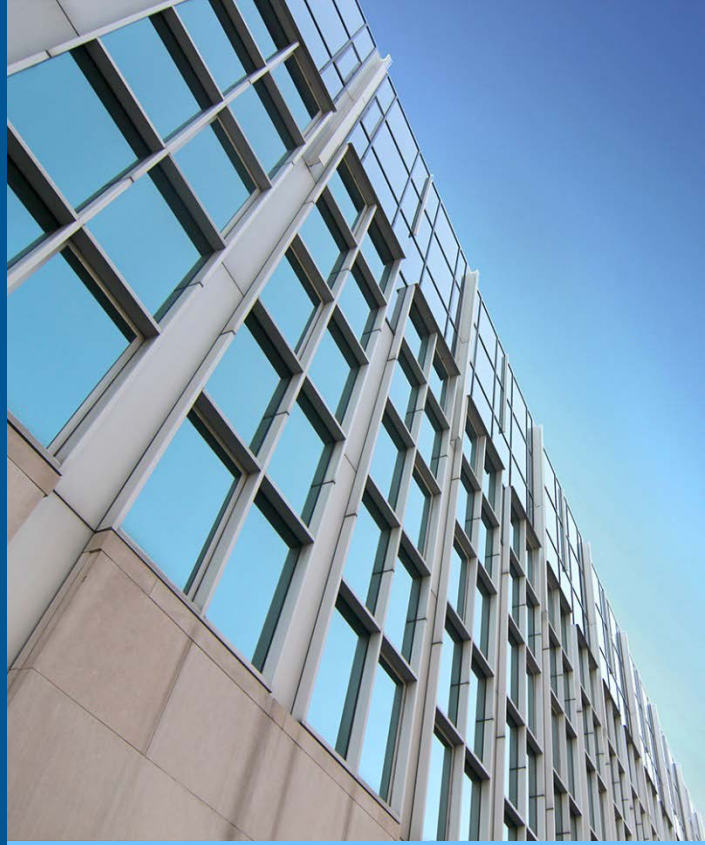
Risk Priority Number: A Method for Defect Report Analysis

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Date: October 2014



Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 OCT 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Risk Priority Number: A Method for Defect Report Analysis	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
William Hayes Julie Cohen /Robert Ferguson	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**55**	

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0001808

Risk Priority Number: A Method for Defect Report Analysis

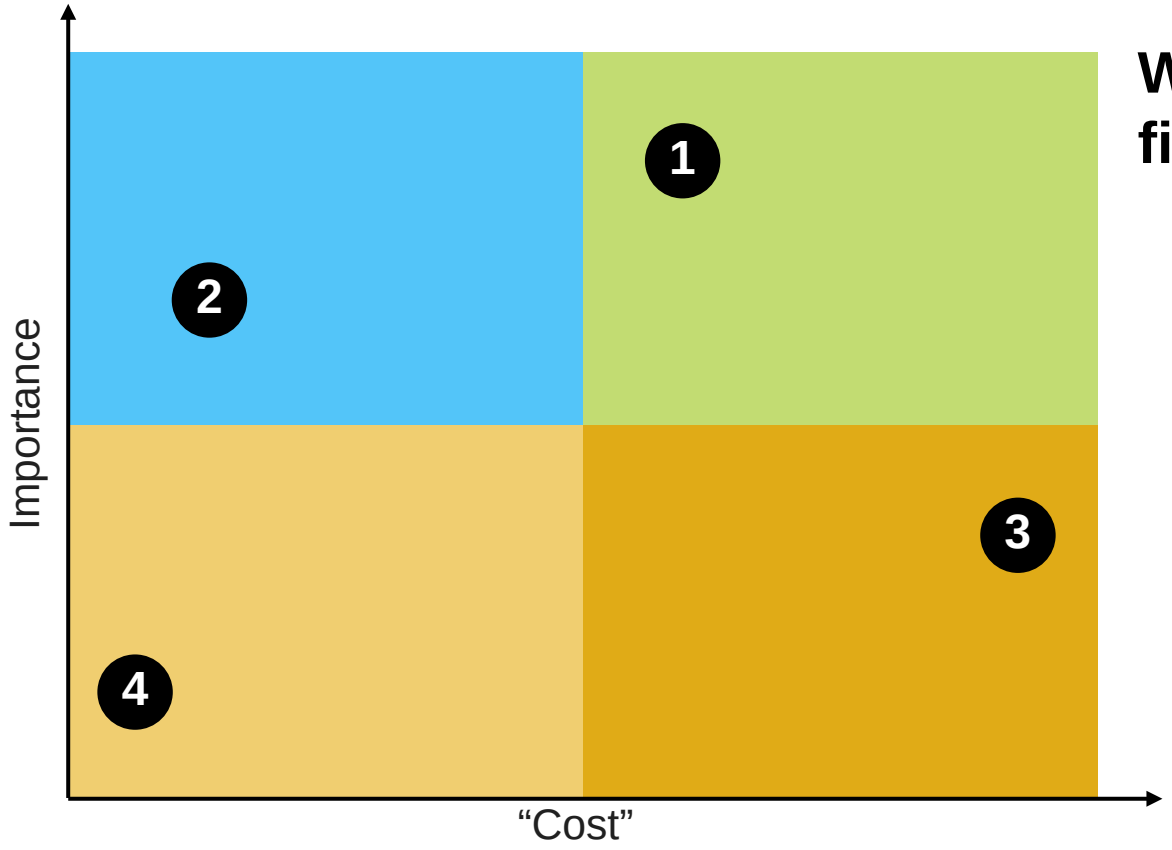
Agenda

General Explanation of Risk Priority Number (RPN)

Suggestions for RPN for DoD Systems Usage

Examples

A Generic Example – Comparing Four Defects



Which would you fix first?

How do we judge importance?

Using “severity” alone has issues

- People are tempted to negotiate a severity rating to account for the importance they perceive
- Without a way to discuss what makes things important, the conversation may become a competition among advocates

RPN focuses on risk exposure

- Allows the team to assess the priority of fixes
- Can relate priority to the understanding of risk

Risk can be perceived from different viewpoints

- User, developer, cost, time
- May need multiple views to make the best decision

RPN General Explanation -1

Generally based on processes that were developed from reliability and cost methods

- **Severity:** a rating of the adverse impact of the defect – a measure that reflects the negative consequence to the users or developers
- **Occurrence:** how often the defect is encountered and/or how long it takes to recover functionality – a measure that reflects a different element of the impact of the defect
- **Detection:** how easy it is to spot the defect is when it occurs – a measure that reflects the risk of unmitigated consequences if the defect is not remedied

RPN General Explanation -2

For weapon systems these may equate to:

- **Severity** = Threat to mission success (Operational and System)
- **Occurrence** = How often it happens, how much time to recover
- **Detection** = Ability to detect that the problem has occurred

RPN General Explanation -3

RPN includes:

- Rating scales characterizing elements of:
  - Severity,
  - Occurrence
  - Detection
- Scaling values for the ratings
- (Optional) Weighting for each rating scale to emphasize what matters most/least in a given system

RPN = Severity x Occurrence x Detection

- A weighted sum, rather than multiplying the numbers together, can be included an option

Polling Question

Would you like us to explain the basic premise of RPN in greater detail?

- Yes
- No

Risk Priority Number:
A Method for Defect Report Analysis

Expected Range of Application

Development, operation, and sustainment contexts are all candidates for adapting RPN to support decision making on which defects to fix first

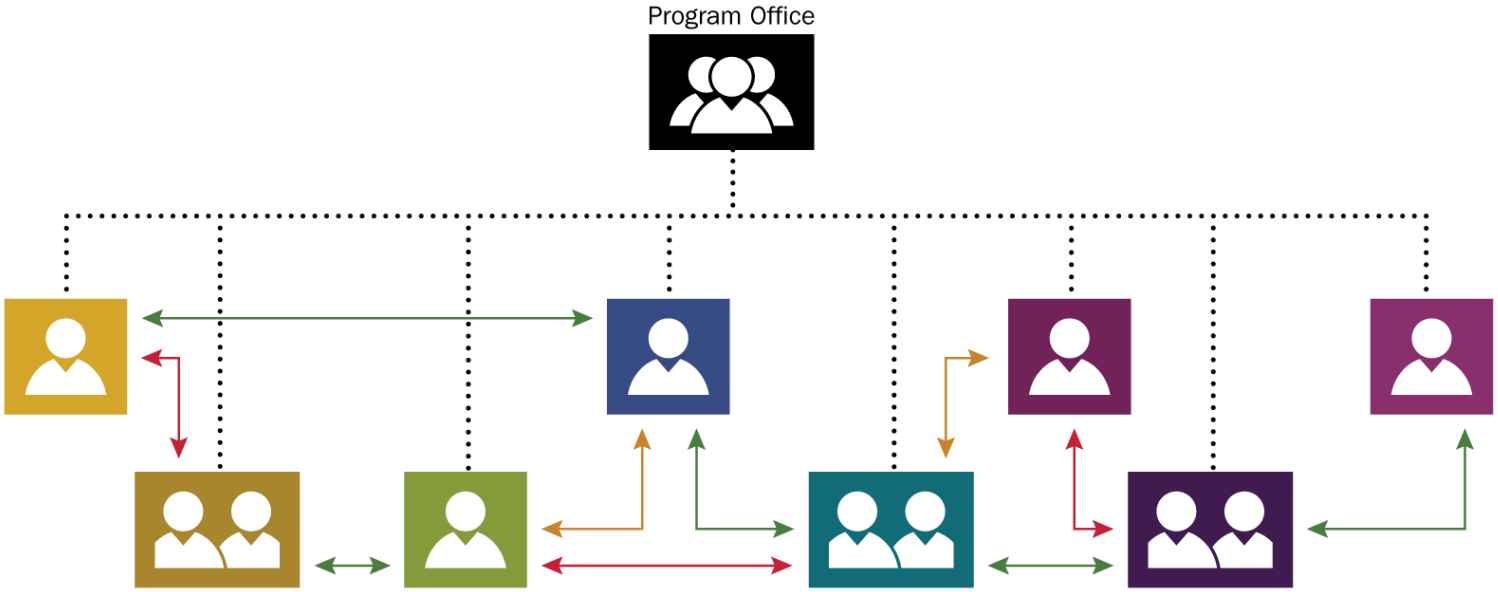
Keys to successful usage

- Custom rating scales developed with appropriate personnel
- Socializing draft materials with stakeholders
- Buy-in from participants in existing defect review processes

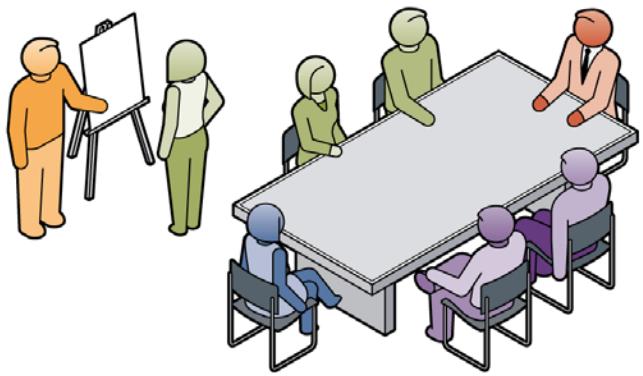
Example Usage – scenario

A major weapon system in early fielding is looking for a way to plan the contents of releases comprised of DR fixes

- Diverse user community with legitimate competing priorities
- Limited funding for future work (many DRs will never be fixed)
- Program office motivated to maximize system utility/value

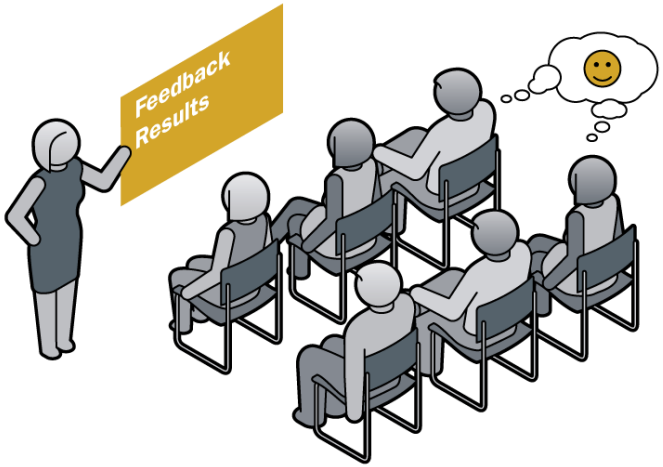


Example Usage 1



1. A small working group was formed
   - Representatives familiar with existing DRs for this system
   - A member of the program office staff who understands the vision for the system
   - Measurement coach who can help navigate the process of constructing measurement scales
   - Draft rating scales were developed as well as computation procedures

Example Usage – 2



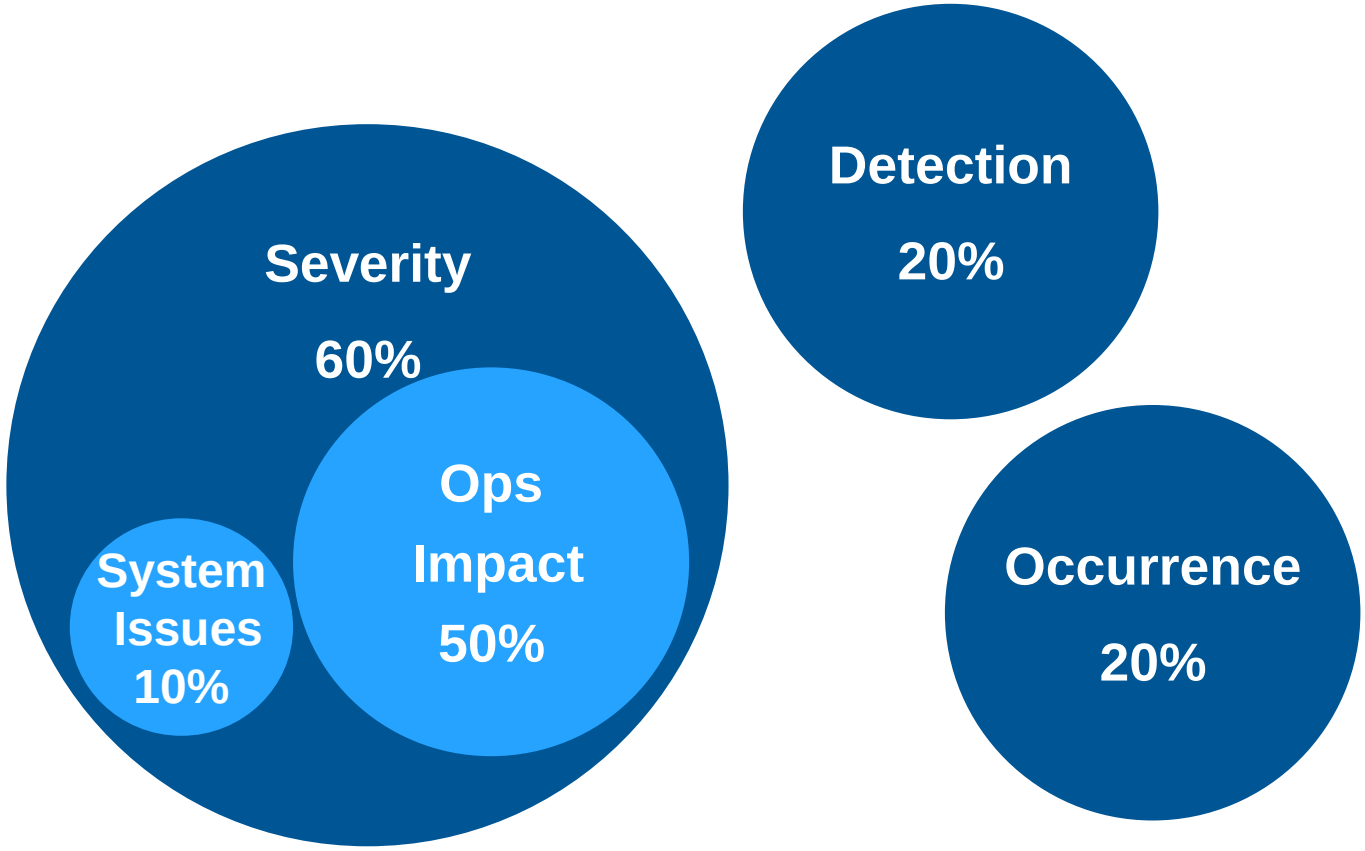
3. Draft materials were reviewed with user communities
   - The reasons for using RPN were explained and tied to the current decision processes
   - The rating scales were explained to people who write DRs or who champion DRs to be included in releases
   - Worked examples of real defects to discuss how ratings are assigned

4. Rating scales and procedures were updated based on feedback

Risk Priority Number:
A Method for Defect Report Analysis

Sample Scales

The following example covers scales developed to fit a specific context, with active involvement of stakeholders.



Rating Scales – Severity – System Function

1		Minor System Malfunction
2		System Malfunctions or Fails to Execute Some Functions but work-around exists
3		Interruption in System Functionality Requiring operator intervention
4		Interruption in System Functionality Requiring contractor Intervention
5		Severely Constrained System Functionality—difficult work-arounds needed
6		No functionality is available and task cannot be performed by any method.
		N/A

Rating Scales – Severity - Operational Impact

1		Increases operator workload slightly
2		Increases operator workload significantly
3		Could limit/delay mission operations
4		Certain delay/limit to mission operations
5		Could cause mission failure
6		Certain mission failure
		N/A

Rating Scales – Detection

1		There is an explicit alert or warning that there is a malfunction; or the system or application fails or crashes.
2		Users will always notice a visible malfunction, and only novices would fail to detect the unexpected system behavior.
3		Users will always notice a visible malfunction, but only after other functions or workflow steps have completed.
4		A user may detect subtle symptoms during normal operation, but may not immediately recognize the cause.
5		Issue not detectable during normal operation

Rating Scales – Occurrence

1		Under 10 hours to recover
2		Less than a week to recover
3		About a week to to recover
4		Weeks to months to recover
5		Up to 3 months to recover
6		More than 3 months to recover

Note: Occurrence = Number of times the defect is encountered per year x the time restore functionality

Polling Question 2

We discussed two scales that equated to Severity – you could use additional scales for other forms of severity and you could also use multiple scales for detection or occurrence.

Would you like to see more examples of these types of scales or continue on to how these scales are used?

- More examples
- Continue

Using Proportional Scales

RPN is based on the use of proportional scales

The ordinal discussed in the last few slides must be changed to a proportional rating

RPN – An Example – Weighted Average

Based on user input the final weighed average was:

Scaled System Behavior rating scale value * 10% +

Scaled Operational Impact scale value * 50% +

Scaled Detection rating scale value * 20% +

Scaled Time scale value * 20%

Resulted in a non-continuous rating scale from 0 to 2400

Note: The four values could also have just been multiplied together, using different scales to adjust for importance

Polling Question

Would you like us to discuss the use of proportional scales and ways to combine the scales or continue with a discussion of how to use the RPN numbers

- More discussion of scales
- Continue with how to use the RPN numbers

Risk Priority Number:
A Method for Defect Report Analysis

Resource Available

For a more complete discussion of the examples presented here, please download the white paper available at the following URL:

http://resources.sei.cmu.edu/asset_files/whitepaper/2013_019_001_70276.pdf

Sample Data Description

For the sample data we have:

Three users – A, B, and C with 10 DRs each

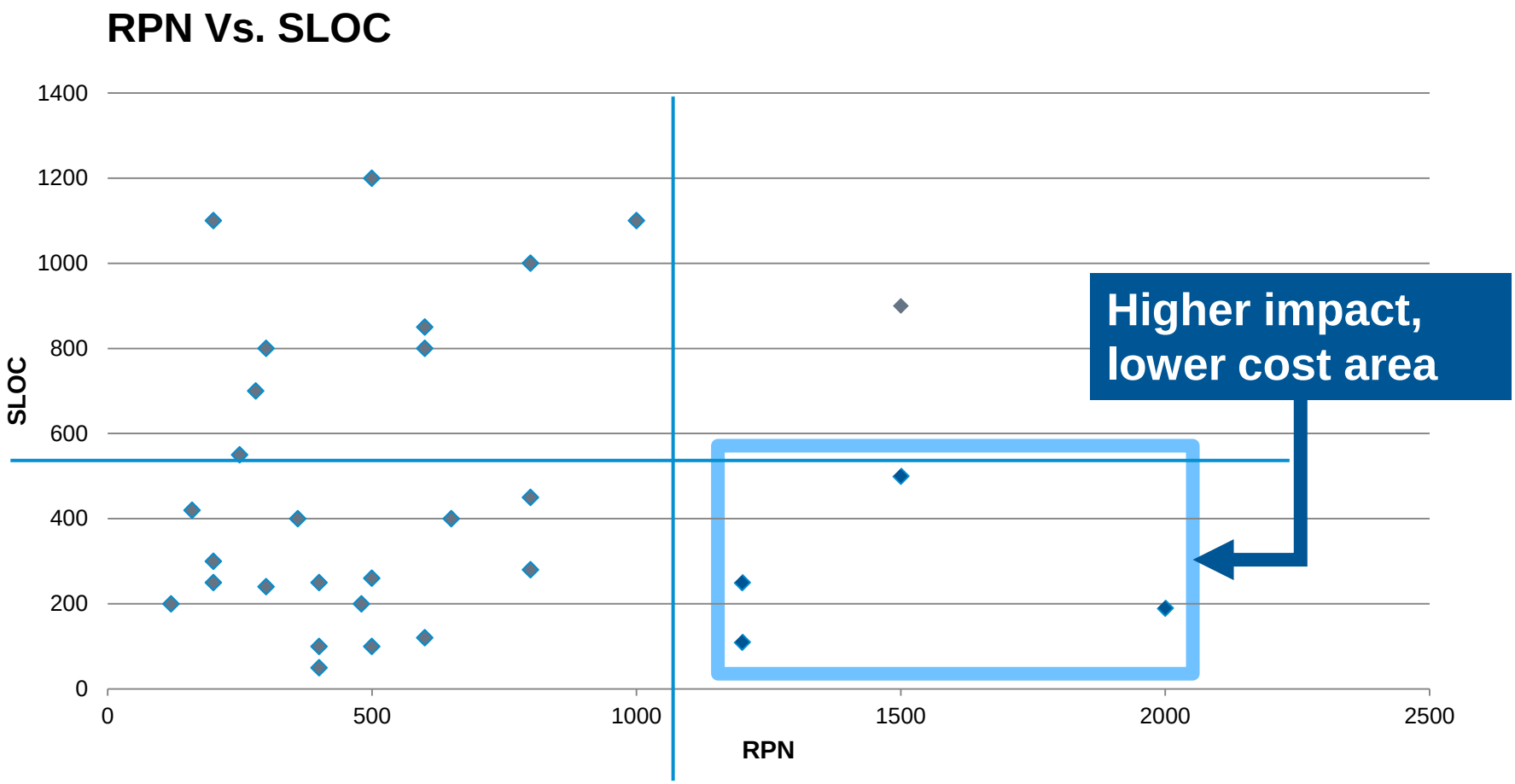
Five Functions

- Communications
- Navigation
- Planning
- Propulsion
- Security

Assume DRs will be fixed in increments of 3,000 Source Lines Of Code (SLOC) each (Note: SLOC is used as a proxy for cost)

Even with this small sample there are hundreds of combinations!

One way to look at the sample data



Note: In this example, SLOC is being used as a proxy for cost

Four Analysis Methods

Method	Brief Description	Pros	Cons
Functionality	Group DRs by system function using RPN and SLOC to select order	- Easier to test specific functional areas - Should see improvements in specific areas addressed	- May not address top user ranked DRs - Some functional areas will not be addressed in every increment - Some functional areas may still need to be split due to SLOC constraints
System Risk	List DRs by RPN and draw a line at the 3000 SLOC; Best used for pure maintenance (regression testing only)	- Addresses system level risk first - Fairly easy to use	- Doesn't specifically address functionality groups - Doesn't specifically address user rankings
User rankings	List DRs by user rankings and draw a line at 3000 SLOC;	- Addresses user rankings - Fairly easy to use	- May fix DRs with lower overall system risk earlier; Doesn't address system value - Doesn't specifically address functionality groups - Need to address differences between users
Hybrid	Combinations of the methods above	Depends on method	Depends on method

Analysis Method - Functionality

Look at top level data in a summary format (30 DRs from 3 Users)

Functional Area	DRs	Total SLOC	Total RPN
Communications	7	2200	5240
Navigation	7	1700	4210
Planning	8	4700	3620
Security	5	3550	2720
Propulsion	3	1450	2100
		13600	

Highest RPN areas are Communications and Navigation

Assuming 3000 SLOC per build you could close all the DRs in Communications, but you will need to do a partial fix in the Navigation Area

Draft Analysis Method - Functionality

DR#	User Priority	Area	SLOC	RPN
120	A2	Communications	250	1200
114	A3	Communications	1000	800
116	B5	Communications	200	2000
121	A6	Communications	100	200
100	A8	Communications	400	160
123	B8	Communications	50	400
115	C9	Communications	200	480
102	B1	Navigation	500	1500
106	B2	Navigation	100	600
107	B3	Navigation	250	200
108	B6	Navigation	100	250
122	B7	Navigation	100	500
101	B9	Navigation	400	360
117	B10	Navigation	250	800
			3900	

User Top 3 Priority

RPN >1000

RPN <500

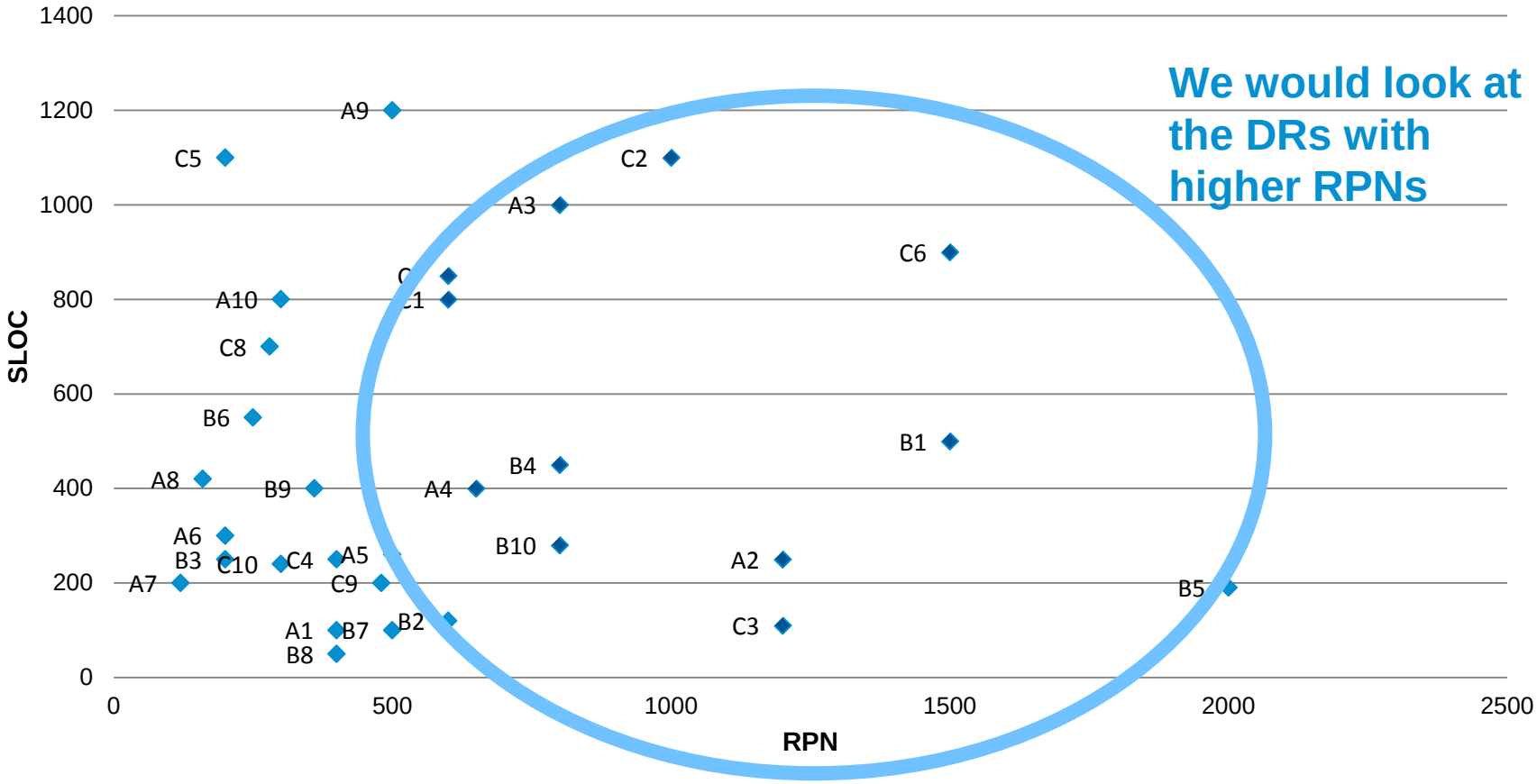
SLOC > 500

3,000 SLOC Cut-Off

First Build - 4 of 9 Top 3 User Rankings, All Comm DRs, First 2 Navigation DRs ; All 3 Users have at least 1 DR fixed

Second Analysis Method – System Risk

RPN vs. SLOC



Top 10 RPN DRs

DR #	User Priority	Area	SLOC	RPN
116	B5	Communications	200	2000
102	B1	Navigation	500	1500
113	C6	Security	900	1500
120	A2	Communications	250	1200
103	C3	Propulsion	400	1200
114	A3	Communications	1000	800
117	B10	Navigation	250	800
125	B4	Security	450	800
118	C2	Planning	1100	800
106	B2	Navigation	100	600
			5150	

User Top 3 Priority

RPN >1000

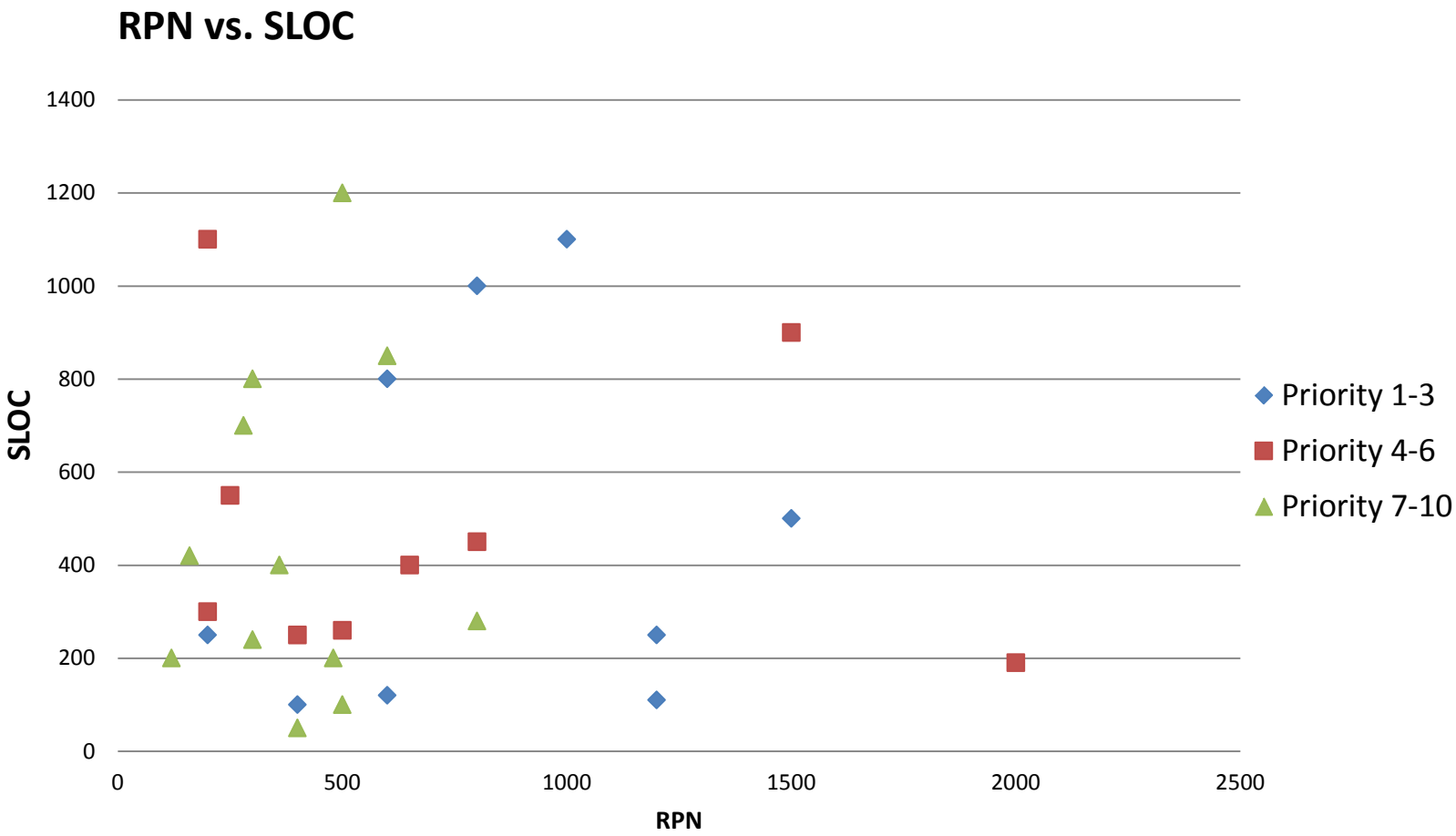
RPN <500

SLOC > 500

3,000 SLOC Cut-Off

First Build - 3 of 9 Top 3 Priority DRs, 4 of 5 functions, burns down ~40% of total system risk

Third Analysis Method – User Ranking



Concentrate on the blue diamonds first

Top User Ranked DRs

DR #	User Priority	Area	SLOC	RPN
124	A1	Planning	100	400
102	B1	Navigation	500	1500
127	C1	Propulsion	800	600
120	A2	Communications	250	1200
106	B2	Navigation	100	600
118	C2	Planning	1100	800
114	A3	Communications	1000	800
107	B3	Navigation	250	200
103	C3	Propulsion	400	1200

User Top 3 Priority

RPN >1000

RPN <500

SLOC > 500

3,000 SLOC Cut-Off

First Build - 6 of 9 Top 3 Priority DRs, 4 of 5 functions

Hybrid Method – Start with User Ranking

DR #	User Priority	Area	SLOC	RPN
124	A1	Planning	100	400
102	B1	Navigation	500	1500
127	C1	**Propulsion**	800	600
120	A2	Communications	250	1200
106	B2	Navigation	100	600
118	C2	Planning	1100	800
114	A3	Communications	1000	800
107	B3	Navigation	250	200
103	C3	**Propulsion**	400	1200
126	A4	Security	400	100
125	B4	Security	450	800
129	C4	Planning	250	400

User Top 3 Priority

RPN >1000

RPN <500

SLOC > 500

Based solely on User Rankings you would fix all the users' top 2 DRs - <u>BUT</u>

Hybrid Method – Then Consider Functionality

Look at top level data in a summary format (30 DRs from 3 Users)

Functional Area	DRs	Total SLOC	Total RPN
Communications	7	2200	5240
Navigation	7	1700	4210
Planning	8	4700	3620
Security	5	3550	2720
Propulsion	3	1450	2100
		13600	

Based solely on User Rankings you would fix all the users' top 2 DRs - BUT

There are only 3 Propulsion DRs total and 2 were top-3 priority list – the total SLOC for all three is 1450 so you might consider doing those first

Hybrid Method – Determine What Else To Include

Based solely on User Rankings you would fix all the users top 2 DRs - BUT

There are only 3 Propulsion DRs total and 2 are in this list – the total SLOC for all three is 1450 so you might consider doing those first

You could then add in 6 of the 7 Navigation DRs and still be under the 3000 SLOC budget

Hybrid Method – Final Listing

DR #	User Priority	Area	SLOC	RPN
127	C1	Propulsion	800	600
103	C3	Propulsion	400	1200
112	C10	Propulsion	250	300
102	B1	Navigation	500	1500
106	B2	Navigation	100	600
107	B3	Navigation	250	200
108	B6	Navigation	100	250
122	B7	Navigation	100	500
117	B10	Navigation	250	800

User Top 3 Priority

RPN >1000

RPN <500

SLOC > 500

Based solely on User Rankings you would fix all the users top 2 DRs - <u>BUT</u>

There are only 3 Propulsion DRs total and 2 are in this list – the total SLOC for all three is 1450 so you might consider doing those first

You could then add in 6 Navigation DRs and 1300 SLOC (2750 total SLOC)

Note: You could add additional DRs to get to 3000 SLOC; or you could have considered adding Communication DRs next instead of Navigation

Other uses

Can be used in a development environment:

- Severity can be related to test blockers or number of interfaces to other units, to key requirements or to operational impacts (if known)
- Detection still based on ability to know the defect has occurred
- Time can be based on the effort needed to correct the defect
- RPN can still be compared to functionality and to total cost to fix

Can be used in a maintenance environments

- Rating scale development would be very similar to the example
- Would tend to try to fix the highest RPN defects first, but may still group by functionality or users depending on the situation

Suggestions for DoD Usage

Develop a team to put together the structure for RPN use

- Include the program office, using command, users, contractors, etc. as needed

Need to develop:

- Definitions for severity which may include different categories
- Definitions for detection which may include different categories
- Methods for dealing with occurrence measures
- Scaling factors
- Computation methods
- Data collection methods
- Process for using RPN values

Questions?

Contact Information

Presenter / Point of Contact

Julie Cohen
Client Technical Solutions Division
Telephone: +1 412.268.3950
Email: jcohen@sei.cmu.edu

William Hayes
Client Technical Solutions Divisions
Telephone: + 1 412.268.6398
Email: wh@sei.cmu.edu

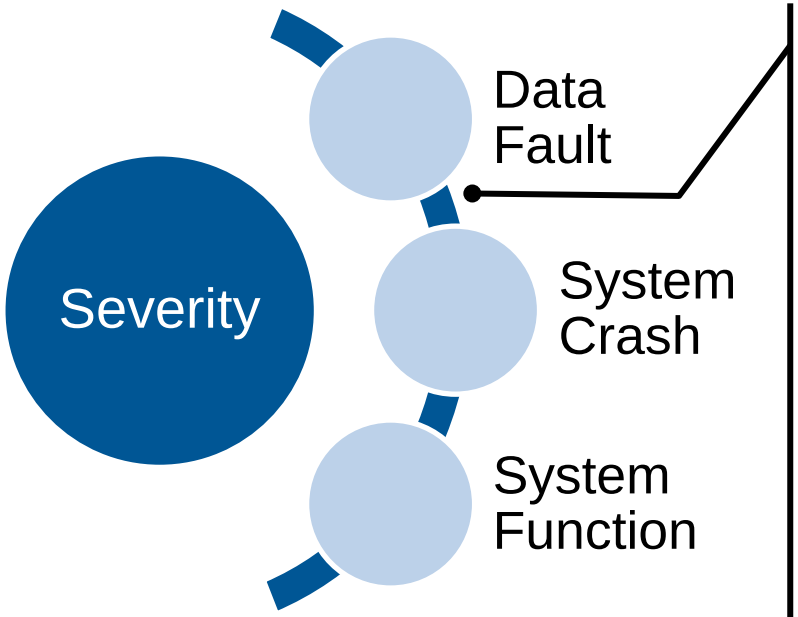
Customer Relations

Email: info@sei.cmu.edu
Telephone: +1 412.268.5800
SEI Phone: +1 412.268.5800
SEI Fax: +1 412.268.6257

Additional Rating Scale Examples

Backup Materials

Rating Scales – Severity



a-1 Minor Data Issue

a-2 Missing Important or Incorrect Data recoverable without using manual changes of data products

a-3 Missing important data or some data incorrect -recoverable using manual changes of data products

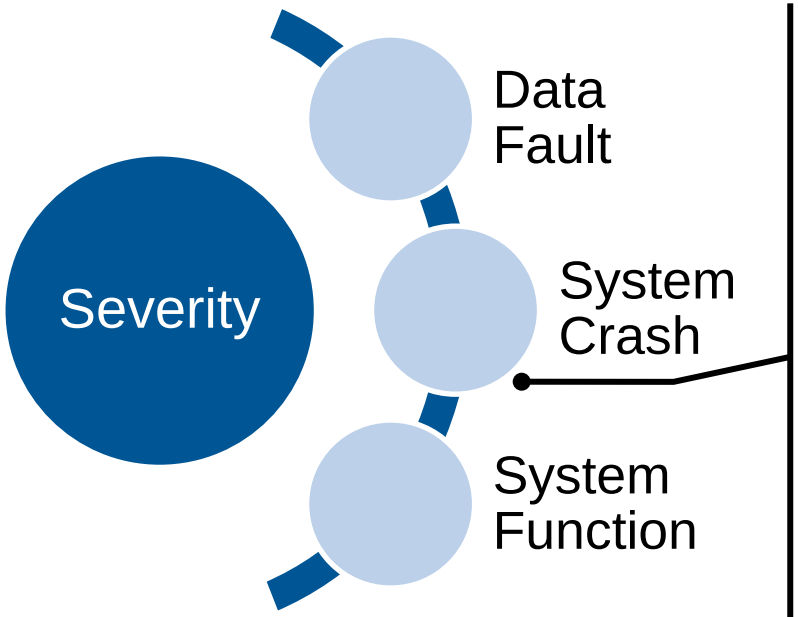
a-4 Missing important data or some data incorrect but some data is fine – non-recoverable

a-5 Recoverable Corruption using manual changes of data products

a-6 Unrecoverable Corruption

N/A

Rating Scales – Severity



b-1 Crash – automatic restart

b-2 Recoverable Application Crash - Simple Recovery

b-3 Recoverable Application Crash - Complex Recovery

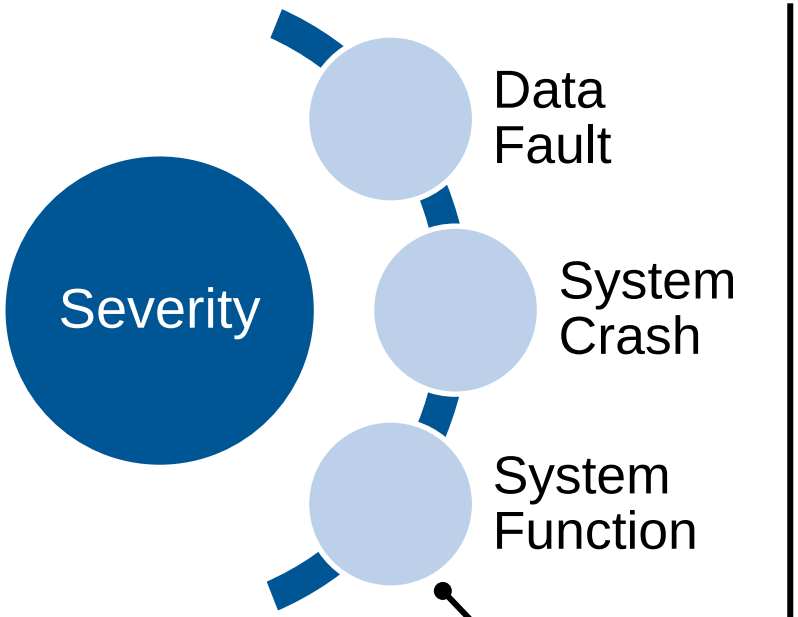
b-4 Recoverable System Crash - Simple Recovery Steps –

b-5 Recoverable System Crash - Complex Recovery Steps

b-6 Unrecoverable System Crash

N/A

Rating Scales – Severity



c-1 Minor System Malfunction

c-2 System Malfunctions or Fails to Execute Some Functions but work-around exists

c-3 Interruption in System Functionality Requiring operator intervention

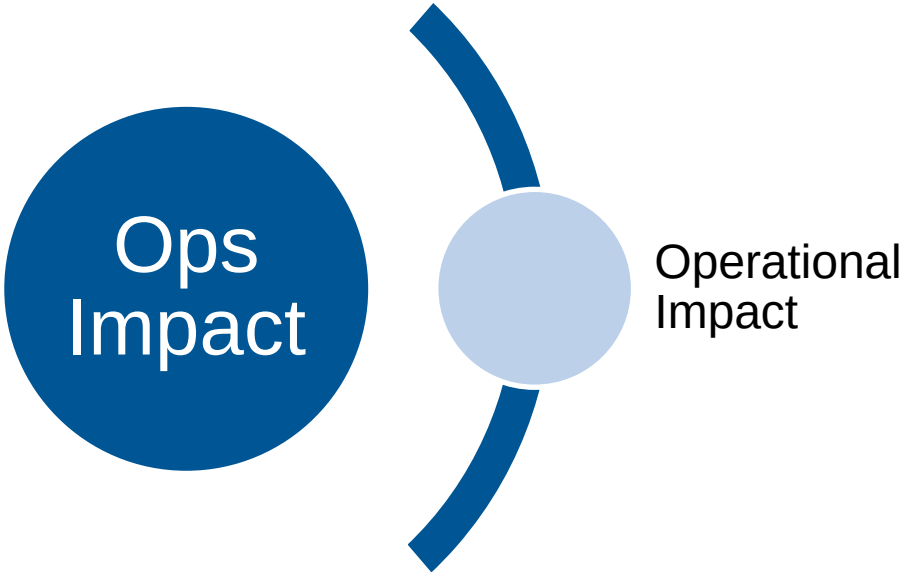
c-4 Interruption in System Functionality Requiring contractor Intervention

c-5 Severely Constrained System Functionality – difficult work-arounds needed

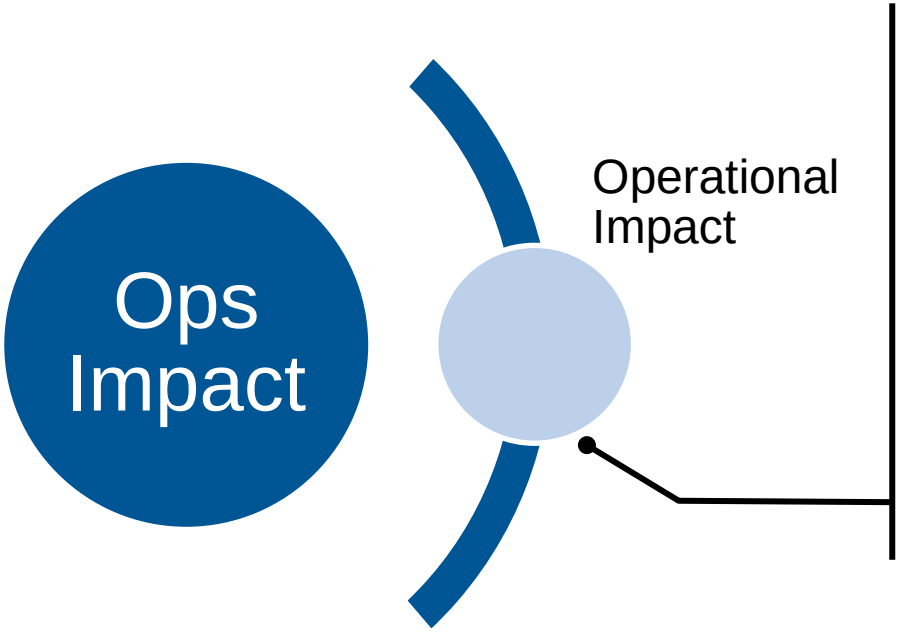
c-6 No functionality is available and task cannot be performed by any method

N/A

Rating Scales – Operational Impact



Rating Scales – Operational Impact



d-1 Increases operator workload slightly

d-2 Increases operator workload significantly

d-3 Could limit/delay mission operations

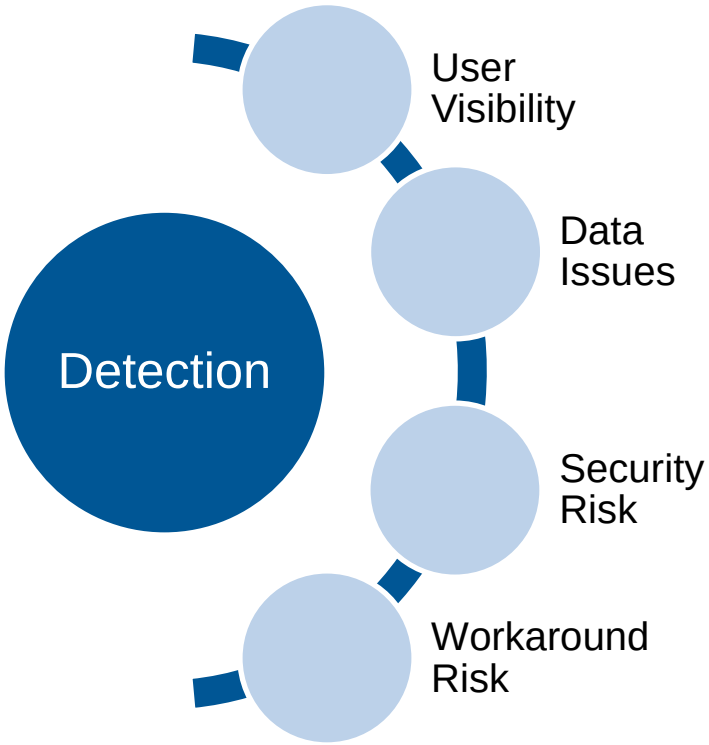
d-4 Certain delay/limit to mission operations

d-5 Could cause mission failure

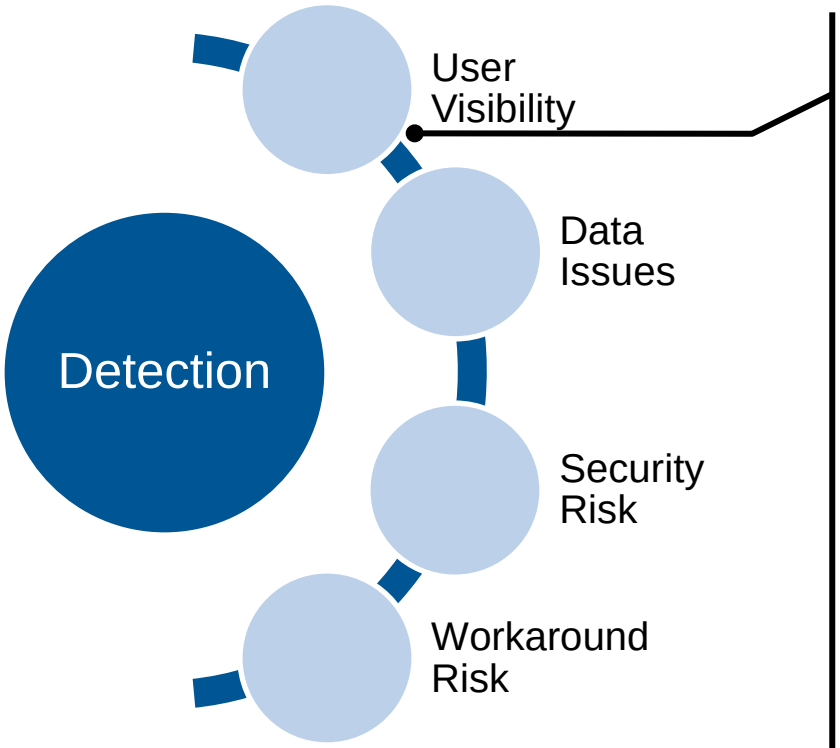
d-6 Certain mission failure

N/A

Rating Scales – Detection



Rating Scales – Detection



e-1 There is an explicit alert or warning that there is a malfunction. Or the system or application fails or crashes.

e-2 Users will always notice a visible malfunction, and only novices would fail to detect the unexpected system behavior.

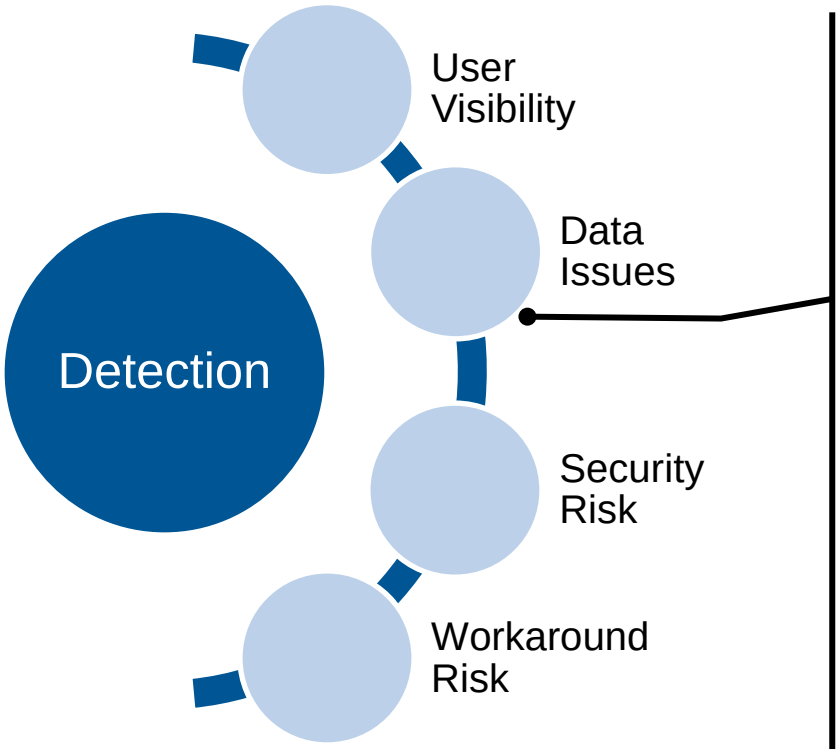
e-3 Users will always notice a visible malfunction, but only after other functions or workflow steps have completed.

e-4 A user may detect subtle symptoms during normal operation, but may not immediately recognize the cause.

e-5 Issue not detectable during normal operation

N/A

Rating Scales – Detection



f-1 The system provides a warning or alert that data corruption has occurred.

f-2 There is data corruption which is revealed to the user by an obvious malfunction or erroneous system output.

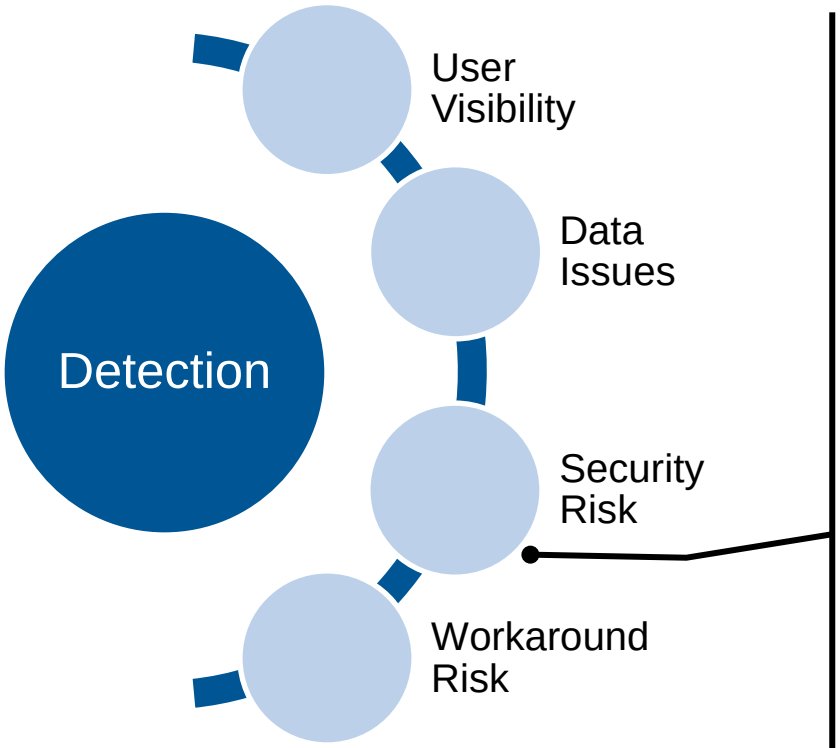
f-3 There is data corruption visible only after a system function or workflow step have revealed the corruption.

f-4 There is a data corruption which can be detected only by specialized staff (e.g., expert user)

f-5 There is data corruption that remains undetectable to the user.

N/A

Rating Scales – Detection



g-1 The system provides a warning or alert regarding the security issue.

g-2 There is a visible security issue which is easily detected by the user.

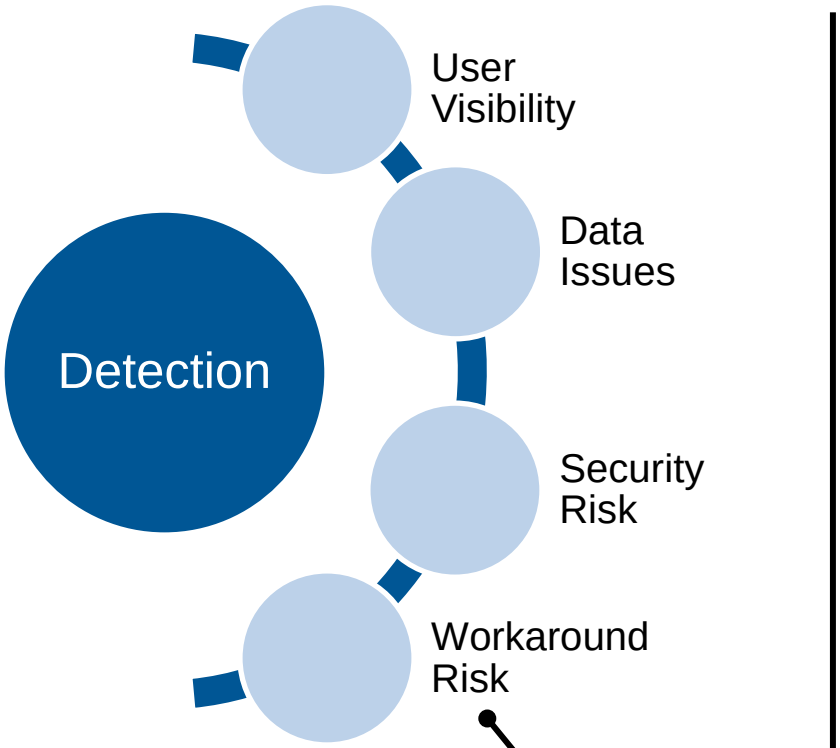
g-3 There is a security issue which can be detected, but only after another system function or workflow step has completed.

g-4 There is a security issue which can be detected, but only with involvement of specialized staff (e.g., expert user),

g-5 There is a security issue which is not visible to the user

N/A

Rating Scales – Detection



h-1 The work-around impacts large areas of system function, so an unsuccessful work-around has greater impact

h-2 The work-around requires specialized expertise to accomplish which may not be readily available when needed

h-3 Work-around implementation blocks all other work on the MPE system (for example, planning can't continue while a crypto work-around is being implemented)

h-4 The workaround requires changes in more than one part of the workflow to be accomplished to ensure the work-around is effective

h-5 Work-around is very error prone and there is high probably that the work-around will be ineffective or will cause unanticipated side-effects that will negatively impact operations

N/A